

**IN THE CLAIMS:**

Please add new claims 13 through 17. Please amend the following claims as indicated. This listing of claims replaces all prior versions, and listings of claims in the application.

1. (Currently amended) A controlled multicast system, including an Ethernet switch and a multicast router, where the Ethernet switch connects with each host ~~of a user~~ in a downlink, connects with the multicast router in an uplink, the multicast router connects with a multicast router of other systems in the uplink, the Ethernet switch implementing multicast exchange of a layer 2, an IGMP V2 protocol is adopted as group management protocol between the Ethernet switch and the host ~~of the user~~; wherein the controlled multicast system further comprises:

a portal server, connecting with the multicast router and providing an interface of user access authentication; and an AAA-authentication server, storing configuration of privilege for the host which wants to join in the multicast group;

The multicast router and the authentication server adopting a Client-server structure by which the authentication server authenticates identification of the host to join in a multicast group with information inputted through the interface provided by the portal server, and the multicast router records a User ID and a corresponding vlan ID of the authenticated host and then distributes control commands according to results of the authentication to control multicast forwarding operations of the Ethernet switch.

~~That connect with the multicast router; the portal server acting as an interface of user access authentication, the AA server being used for storing configuration of privilege for the user to join in a multicast group; the multicast router cooperating with the AAA server together to implement privilege authentication for the user to join in the multicast group, and distributing control commands according to results of the authentication to control multicast forwarding operations of the Ethernet switch.~~

2. (Currently amended) The controlled multicast system according to claim 1, a RADIUS+ protocol extended from an RADIUS (Remote Authentication Dial In User

Service) ~~AAA~~ protocol is adopted as communication protocol between the multicast router and the authentication ~~AAA~~ server; ~~a group management protocol HGMP (Huawei Group Management Protocol)~~ is used as a control protocol between the ~~Ethernet switch~~ and the multicast router.

3. (Currently amended) The controlled multicast system according to claim 1,  
wherein the authentication server is an AAA (authorization and Authentication) server. A  
method for implementing a controlled multicast, comprises: implementing access  
authentication first; then an Ethernet switch classifying a vlan according to a port and  
handling an IGMP message from a host, implementing user identification authentication for  
joining in a multicast group, and a multicast router handling the IGMP message; in  
succession, the multicast router controlling the Ethernet switch for multicast forwarding,  
between which the HGMP protocol is used as a control protocol of the controlled multicast;  
after that, the Ethernet switch disposing a HGMP control message and forwarding a multicast  
flow; the host leaving the multicast group and making corresponding processes after finishing  
the forwarding operation.

4. (Currently amended) The controlled multicast system according to claim 1,  
wherein configuration of privilege comprises a corresponding relation between the User ID of  
the host and an address of multicast group in which the host wants to join;

the information inputted through the interface provided by the portal server comprises  
the User ID and a password;

each port through which the host is connected to the Ethernet switch is a vlan port;

wherein the authentication server in the system further for, after receiving an extended  
RADIUS authentication message from the multicast router, of which attributes include the  
User ID as the user name and the address of multicast group in which the host wants to join,  
detecting whether to accept the host joining in the multicast group based on the configuration  
of privilege;

responding with an acceptance message to the multicast router if the host has suitable  
privilege, otherwise returning a reject message;

wherein the multicast router in the system further for, after receiving an IGMP Membership Report message from the Ethernet switch, according to the vlan ID in the message, searching the corresponding User ID in a multicast access privilege table of the multicast router, and then sending the said extended RADIUS authentication message, to the authentication server;

after receiving the acceptance message from the authentication server, writing the address of the multicast group in which the host can join into the said multicast access privilege table, and implementing a routine disposal on join messages of the host, then generating a Join message, which comprises the vlan ID corresponding to the port that links with the host which wants to join in the multicast group, the address of the multicast group that is applied for, and a Join command field, and then transmitting to the Ethernet switch; moreover, completing a routine processing of creating multicast forwarding tree on the IGMP Membership Report message; doing nothing after receiving the reject message;

the Ethernet switch for, forwarding the IGMP Membership Report message from the host, wherein the IGMP Membership Report message forwarded to the multicast router port carries with the vlan ID of the host;

after receiving the Join message from the multicast router, searching the MAC address corresponding to the address of the multicast group in the forwarding table; if the entry corresponding with the MAC address is found, obtaining the port number of the host via searching in the forwarding table with the vlan ID in the Join message, and then adding the port number into the said entry; if nothing is found, adding an entry in the forwarding table, which comprises the MAC address corresponding to the multicast address, the port number of the host which applies to join in the multicast group, and the port number of the multicast router connected with the Ethernet switch;

after receiving a multicast flow from the multicast router, forwarding it to ports of the Ethernet switch with the current forwarding table.~~The method according to claim 3, wherein the step of implementing access authentication comprises:~~

~~(1) —when accessing a network, the host inputting an authentication information that includes a User ID and a password first through an interface provided by a portal server, and a AAA server authenticating identification of the host with the information; once the~~

~~authentication is successful, the multicast router recording the User ID and a corresponding vlan ID of the host in a multicast access privilege table of the user;~~

~~the step of the Ethernet switch classifying the vlan according to the port and handling the IGMP message from the host comprises,~~

~~(2) — classifying the vlan according to the ports, with one vlan for each port, and linking one port to one host; searching a Content Addressable Memory (CAM) table with a destination MAC address of the IGMP message sent by the host and forwarding the said IGMP message, of which forwarding process is same with that of a unicast message: if the port corresponding to the destination MAC address is found, forwarding the multicast message to the port, otherwise forwarding the multicast message to all the ports;~~

~~the step of implementing user identification, authentication for joining in the multicast group, and handling the IGMP message by the multicast router comprises,~~

~~(3) — after receiving an IGMP Membership Report message, according to the vlan ID in the message, the multicast router finding the corresponding USER ID and the host to which the IGMP Membership Report message belongs through searching in the multicast access privilege table of the user recorded in step (1), and then sending an extended RADIUS authentication message which includes the user ID just found as the user name and the address of multicast group in which the host wants to join as an attribute, to the AAA server for authentication;~~

~~the AAA server determining whether to accept the user based on services of the user; if the user has the suitable privilege, responding with an acceptance message, otherwise returning a reject message; after receiving the reject message, the multicast router do nothing, but if receiving the acceptance message, the multicast router writing the address of the multicast group in which the user can join into the multicast access privilege table of the user, and implementing a routine disposal on join messages of the host, then generating and transmitting a HGMP Join message to the Ethernet switch, which comprises the vlan ID corresponding to the port that links with the host which wants to join in the multicast group, the address of the multicast group that is applied for, and a Join command field; moreover, the multicast router also completing a routine processing of creating multicast forwarding tree on the IGMP Membership Report message just like an ordinary multicast router does;~~

~~(4) — managing generation and deletion of an entry in the CAM table at the Ethernet switch by the multicast router; while allowing the host to join in the multicast group, the multicast router sending the HGMP join message that includes the vlan ID of the host which applies to join in the multicast group and the address of the multicast group applied for to the Ethernet switch; when the multicast router wants to terminate the host joining in the multicast group, the multicast router transmitting a HGMP Leave message which comprises the vlan ID of the host which leaves the multicast group and the address of the multicast group where the host leaves;~~

~~the step of the Ethernet switch disposing the HGMP control message comprises,~~

~~(5) — after receiving the HGMP Join message, the Ethernet switch searching the CAM table with the MAC address corresponding to the address of the multicast group; if the entry corresponding with the address is found, the Ethernet switch obtaining the port number of the host via searching the CAM table with the vlan ID in the HBMP Join message, and then adding the port number into the said entry; if nothing is found, adding an entry in the CAM table, which comprises the MAC address corresponding to the multicast address, the port number of the host which applies to join in the multicast group, and the port number of the multicast router connected with the Ethernet switch;~~

~~after receiving the HGMP Leave message, the Ethernet switch obtaining the entry through looking up the CAM table with the MAC address corresponding to the multicast address of the multicast group, and getting the port number of the host through searching with the vlan ID, and then deleting the said port number from the said entry, if the said port number is the solely port of the said entry, deleting the whole entry;~~

~~the step of forwarding of the multicast flow comprises,~~

~~(6) — when receiving the multicast flow sent from the multicast source, the multicast router forwarding the multicast flow to an egress based on a CAM table; when handling the IGMP Membership Report message of the host, the multicast router creating a multicast forwarding egress according to the real port of the Ethernet switch, and sending only one copy of the multicast flow to the Ethernet switch;~~

~~the step of the host leaving the multicast group comprises,~~

~~(7) after finishing the multicast and wanting to leave the multicast group, the host sending an IGMP Leave message; after receiving the IGMP Leave message, the multicast router extracting the vlan ID from the message, and obtaining corresponding entry via searching in the multicast access privilege table created in step (1) with the vlan ID, then deleting the address of the multicast group indicated by the IGMP Leave message in the entry; after completing a routine disposal on leave messages, the multicast router generating the IGMP Leave message and sending to the Ethernet switch, which includes the vlan ID of the host which wants to leave group, the address of multicast group where the host wants to leave and a Leave command field.~~

5. (Currently amended) ~~The method according to claim 3, wherein the CAM table and the unicast forwarding table of the Ethernet switch are shared.~~The controlled multicast system according to claim 1, wherein the multicast router in the system further for, after receiving an IGMP Leave message, extracting the vlan ID from the message, and obtaining corresponding entry in the multicast access privilege table via searching with the vlan ID, then deleting the address of the multicast group indicated by the IGMP Leave message in the entry;

after completing a routine disposal on leave messages of the host, generating a Leave message and sending to the Ethernet switch, which includes the vlan ID of the host which wants to leave the multicast group, the address of multicast group where the host wants to leave and a Leave command field;

the Ethernet switch further for, after receiving the Leave message from the multicast router, obtaining the entry through looking up the forwarding table with the MAC address corresponding to the multicast address of the multicast group, and getting the port number of the host with the vlan ID in the Leave message, and then deleting the said port number from said entry.

6. (Currently amended) ~~The method according to claim 3, wherein, during the messages forwarding, adopting a vlan protocol between the port of the multicast router and the Ethernet switch.~~The controlled multicast system according to claim 1, wherein the multicast router in the system further for, after knowing offline status of the host, actively

generating the Leave message and sending to the Ethernet switch; moreover terminating the multicast flow transmission.

7. (Currently amended) ~~The method according to claim 3, in step (6) there is no~~  
~~vlan ID in a multicast data packet of the multicast flow sent from the multicast router.~~A  
method for implement a controlled multicast, comprising:

A. in advance, according to ports of an Ethernet switch, classifying vlan with one  
vlan for each port, and linking one port to the host;

making access authentication for a host which wants to join in a multicast group, if  
the authentication is successful, executing step B, otherwise ending;

B. forwarding an IGMP Membership Report message from the host by the  
Ethernet switch;

C. detecting whether to accept the host joining in the multicast group, if it is,  
generating a Join message to control establishing of an entry in a forwarding table of the  
Ethernet switch by a multicast router, and forwarding a multicast flow from the multicast  
router according to the current forwarding table by the Ethernet switch; otherwise ending.

8. (Currently amended) ~~The method according to claim 3, in step (7) of leaving~~  
~~from the multicast group can also be implemented via following means which comprises,~~  
~~once the multicast router knows offline status of the user, the multicast router actively~~  
~~sending the IGMP Leave message to terminate multicast flow transmission to the host,~~  
~~which is same with that of processing on the IGMP Leave message.~~The method for  
implementing a controlled multicast according to claim 7, for the host which wants to leave  
the multicast group, the method further comprising, forwarding an IGMP Leave message  
from the host by the Ethernet switch; generating a Leave message to control deleting the  
entry of the host in the forwarding table after the multicast router receives the IGMP Leave  
message.

9. (Currently amended) ~~The method according to claim 3, further comprises~~  
~~controlling the multicast sender, which includes when the host transmits data to the multicast~~

~~group, the first receiver among the multicast routers filtering the data message with a multicast Access Control List (ACL), and forwarding the data message that satisfies the requirements in the ACL to the multicast tree.~~The method for implementing a controlled multicast according to claim 7, further comprising, actively generating the Leave message to control deleting the entry of the host in the forwarding table by the multicast router once knowing offline status of the host, and terminating the multicast flow transmission.

10. (Currently amended) ~~The method according to claim 9, wherein the multicast ACL is distributed to each multicast router by a centralized multicast service control server; the step of controlling the sender is accomplished with the multicast ACL by the multicast router, meanwhile the multicast service control server is also acts as the AAA server.~~The method for implementing a controlled multicast according to claim 7, in step A, the said step of making access authentication for a host which wants to join in the multicast group comprises,

in advance, storing configuration of privilege for hosts which want to join in the multicast group in an authentication server that connects with the multicast router, wherein the configuration of privilege includes a corresponding relation between a User ID of the host and an address of multicast group in which the host wants to join;

inputting information including the User ID and a password through an interface provided by a portal server, and authenticating identification of the host with the information by the authentication server;

recording the User ID of the host and a corresponding vlan ID of the host in a multicast access privilege table by the multicast router after the authentication is successful;

the step B further comprises,

if the port corresponding to the destination MAC address in the IGMP Membership Report message is found in the forwarding table, forwarding to the found port, otherwise forwarding to all ports; wherein the IGMP Membership Report message forwarded to the multicast router port carries with vlan ID of the host;

the step C further comprises,



C1. after multicast router receives the IGMP Membership Report message, searching the User ID of the host in the multicast access privilege table based on the vlan ID in the IGMP Membership Report message; then sending an extended RADIUS authentication message which includes the User ID just found as the user name and the address of multicast group in which the host wants to join as the name and the address of multicast group in which the host wants to join as the attribute, to the authentication server; detecting whether to accept the host joining in the multicast group by the authentication server according to the configuration of privilege;

If the host has suitable privilege, responding with an acceptance message to the multicast router by the authentication server, and then executing step C2, otherwise returning a reject message; the multicast router does nothing and ends after receiving the reject message;

C2. after the multicast router receives the acceptance message, writing the address of the multicast group in which the host can join into the said multicast access privilege table, and implementing a routine disposal on join messages of the host, then generating a Join message, which comprises the vlan ID corresponding to the port that links with the host which wants to join in the multicast group, the address of the multicast group that is applied for, and a Join command field, and then transmitting to the Ethernet switch; moreover, completing a routing processing of creating multicast forwarding tree on the IGMP Membership Report message;

C3. searching the MAC address corresponding to the address of the multicast group in the forwarding table by the Ethernet switch; if the entry corresponding with the MAC address is found, obtaining the port number of the host via the vlan Id IN THE Join message, and then adding the port number into the said entry; if nothing is found, adding an entry in the forwarding table, which comprises the MAC address corresponding to the multicast address, the port number of the host which applies to join in the multicast group, and the port number of the multicast router connected with the Ethernet switch;

C4. sending only one copy of the multicast flow to the Ethernet switch by the multicast router.

11. (Currently amended) ~~The method according to claim 9, wherein the multicast ACL is distributed to each multicast router by a centralized multicast service control server; the step of controlling the sender is accomplished with the multicast ACL by the multicast router, meanwhile the multicast service control server is also acts as the AAA server.~~The method for implementing a controlled multicast according to claim 8, the step of forwarding an IGMP Leave message from the host further comprises, forwarding the IGMP Leave message from the host based on the current forwarding table; wherein the IGMP Leave message forwarded to the multicast router carries with the vlan ID of the host;

the step of generating a Leave message to control deleting the entry of the host in the forwarding table further comprises,

after the multicast router receives the IGMP Leave message, extracting the vlan ID from the message, and obtaining corresponding entry via searching in the multicast access privilege table with the vlan ID, then deleting the address of the multicast group indicated by the IGMP Leave message in the entry of the multicast access privilege table; completing a routine disposal on leave messages of the host, and then generating a Leave message and sending to the Ethernet switch, which includes the vlan ID of the host which wants to leave the group, the address of multicast group where the host wants to leave and a Leave command field;

after the Ethernet switch receives the Leave message, obtaining the entry through looking up the forwarding table with the MAC address corresponding to the multicast address of the multicast group, and getting the port number of the host with the vlan ID in the Leave message, and then deleting the said port number from the said entry.

12. (Currently amended) ~~The method according to claim 9, wherein the multicast ACL can also be distributed by a centralized policy server or a network manager.~~The method for implementing a controlled multicast according to Claim 11, the step of generating a Leave message to control deleting the entry of the host in the forwarding table further comprises, if the deleted port is the solely port of the said entry in the forwarding table, further deleting the whole entry.

13. (New) The method for implementing a controlled multicast according to Claim 7 during the messages forwarding, adopting a vlan protocol between the multicast router port and the Ethernet switch.

14. (New) The method for implementing a controlled multicast according to claim 7, the method further comprises, filtering data messages send by a multicast sender with a multicast Access Control List (ACL) through the first receiver among the multicast routers, and forwarding the data messages that satisfy the requirements in the ACL to the multicast tree.

15. (New) The method for implementing a controlled multicast according to claim 14, wherein the multicast ACL comprises a command word, a source address and a group address.

16. (New) The method for implementing a controlled multicast according to claim 14, wherein the multicast ACL is distributed to each multicast router by a centralized multicast service control server; meanwhile the multicast service control server is also acts as the authentication server.

17. (New) The method for implementing a controlled multicast according to claim 14, wherein the multicast ACL can also be distributed by a centralized policy server or a network manager.